Using Discrete-Time Hyperchaotic-Based Asymmetric Encryption and Decryption Keys for Secure Signal Transmission

Sonia HAMMAMI
University of Tunis El Manar
Engineering Sciences
and Techniques Departement
El Manar Preparatory Institute
for Engineering Studies, Tunisia
BP 244, Tunis 2092, Tunisia
sonia.hammami@enit.rnu.tn

Mohamed DJEMAÏ
Univ. Lille Nord
CNRS, UMR-8201, F-59313
Valenciennes, France
UVHC, LAMIH F-59313
Valenciennes, France
mohamed.djemai@univ-valenciennes.fr

Krishna BUSAWON
Northumbria University
Faculty of Engineering
and Environment
NE1 8ST Newcastle Upon Tyne, UK
krishna.busawon@northumbria.ac.uk

***Abstract*— In this paper, a framework for the synchronization of two non-identical discrete-time hyperchaotic systems, namely the 3D Baier-Klein and the 3D Hitzel-Zele maps, based on the use of hybrid output feedback concept and aggregation techniques, is employed to design a two-channel secure communication system. New sufficient conditions for synchronization are obtained by the use of Borne and Gentina practical criterion for stabilization study associated to the forced arrow form matrix for system description. The efficiency of the proposed approach to confidentially recover the transmitted message signal is shown via an application to the hyperchaotic Baier-Klein and Hitzel-Zele systems, considered as generators of asymmetric encryption and decryption keys.**

Index terms – Discrete-time hyperchaotic maps; Hybrid output feedback; Forced arrow form matrix; Synchronization; Asymmetric encryption and decryption keys.

I. INTRODUCTION

Chaos and its applications in the field of secure communication has been the subject of intensive research during the last two decades. Indeed, the pioneering work done in the synchronization of chaotic systems, that was initiated by Pecora and Carroll [1-2], as well as the random-like behaviour of chaotic signals provide the potential for many applications; in particular, the introduction of chaos into secure communication field [3-6]. In recent years, a growing number of cryptosystems based on chaos synchronization have been proposed such as: chaotic masking [7-8], chaotic modulation [9-10], chaotic shift keying [11-12]. In papers [13-16], a novel idea for secure communication was proposed using discrete-time chaotic systems based on encryption, where a different output from chaotic transmitter, which was transmitted in the channel, was used as a key stream to encrypt the message signal.

In this paper, we use secure communication based on encryption using two communication channels, instead of one, for the purposes of fast synchronization and higher security [17]. In these cryptosystems, the cipher text consists of a complex nonlinear combination of the plaintext and a mixture of state variables of a chaotic transmitter's generator. Since it was not possible to synchronize the slave system with such cipher text, a second channel had to be used in the system for transmitting synchronization signal.

Thus, the main purpose of this work is to determine necessary and sufficient conditions for the asymptotic stability of the error states between two different hyperchaotic discrete-time processes. In fact, these processes can, not only reach chaos synchronization starting with different initial conditions, but also can be applied to two secure communication channels based on chaotic systems. The proposed stabilizing conditions for nonlinear discrete-time two levels hierarchical systems are based on the Borne and Gentina practical criterion for stability study [18] associated to the forced arrow form matrix for system description [19-23].

The paper is organized as follows: in Section 2, we proposed a systematic approach to design a hybrid output feedback that is effective in achieving synchronization of discrete-time hyperchaotic systems. Additionally, it guarantees the asymptotic stability for the synchronization errors, characterized in the state space, by a forced arrow form matrix. The implementation of the proposed synchronization scheme to two secure chaotic communication channels, using two non-identical discrete-time hyperchaotic Baier-Klein and Hitzel-Zele systems is realised in Section 3. In Section 4, numerical simulations are carried out using this kind of discrete-time hyperchaotic systems and the proposed secure communication scheme. Finally, some concluding remarks are given.

II. MAIN METHODOLOGY

The proposed synchronization approach for a class of discrete-time hyperchaotic systems for two secure communication channels is illustrated in Figure 1.

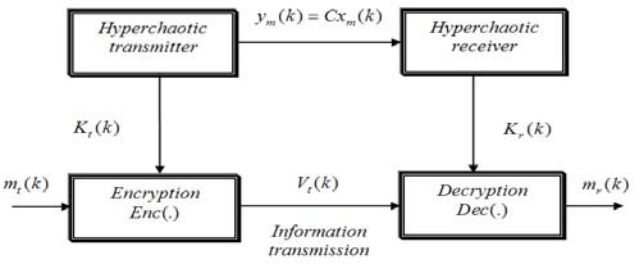

Figure 1. The proposed hyperchaotic communication sheme

A. Hybrid output feedback-based discrete-time hyperchaotic synchronization

Consider the $n-$dimensional hyperchaotic discrete-time in Lurie form master and slave systems.

The master system is modelled as follows:

$$\begin{cases} x_m(k+1) = A_m\left(x_m(k)\right)x_m(k) + \alpha R V_t(k) \\ y_m(k) = C x_m(k) + \alpha V_t(k) \end{cases} \quad (1)$$

where $x_m(kT) \in \mathbb{R}^n$ is the state vector, noted $x_m(k)$ at the instant kT, T the sampling time. $A_m(.) = \left\{a_{mij}(.)\right\}$ the $n \times n$ instantaneous characteristic matrix of (1), $C = \begin{bmatrix} c_1 & \dots & c_n \end{bmatrix}$ a $(1 \times n)$ constant output matrix, $R = \begin{bmatrix} r_1 & \cdots & r_n \end{bmatrix}^T$ a constant vector characterizing the way to mix the cipher text $V_t(k)$ with the chaotic signal $x_m(k)$, and α a scaling factor chosen to allow the term $\alpha R V_t(k)$ belonging to a compatible range with respect to the minimum and maximum bound of states variables of master and slave chaotic signal $V_t(k)$ [24-25].

By referring to the inclusion method [26-27], the considered hyperchaotic master system (1) generates the output signal $y_m(k) \in \mathbb{R}$ and the key $K_t(k)$ used q times as a key stream to encrypt the original message $m_t(k)$ with an encryption rule $Enc(.)$, a $q-$shift cipher algorithm, such as:

$$V_t(k) = Enc\left(m_t(k), K_t(k)\right) = \underbrace{f_1(\dots f_1(}_{q} f_1(m_t(k), \underbrace{K_t(k)), K_t(k)), \dots, K_t(k))}_{q} \quad (2)$$

with:

$$K_t(k) = \sqrt{x_{m1}^2(k) + \dots + x_{mn}^2(k)} \quad (3)$$

$x_{mi}(k),\ \forall i = 1, \dots, n$ are the components of the state vector $x_m(k)$.

$f_1(.)$ is a nonlinear function defined, in this case, by:

$$f_1(m_t(k), K_t(k)) = \begin{cases} m_t(k) + K_t(k) + 2h, & \text{for } -2h \le m_t(k) + K_t(k) \le -h \\ m_t(k) + K_t(k), & \text{for } -h < m_t(k) + K_t(k) < h \\ m_t(k) + K_t(k) - 2h, & \text{for } h \le m_t(k) + K_t(k) \le 2h \end{cases} \quad (4)$$

h is an encryption parameter chosen such that the transmitted message $m_t(k)$ and the key $K_t(k)$ lie within the interval $[-h, h]$. The output signal $y_m(k)$, is sent through the public channel to the bloc operating in the decryption phase.

The hyperchaotic slave system is described by:

$$\begin{cases} x_s(k+1) = A_s\left(x_s(k)\right)x_s(k) + K_y V_r(k) \\ y_s(k) = C x_s(k) \end{cases} \quad (5)$$

$x_s \in \mathbb{R}^n$, $y_s \in \mathbb{R}$ are, respectively, the state vector and the output of the slave system. $A_s(.) = \left\{a_{sij}(.)\right\}$ the $n \times n$ instantaneous characteristic matrix of (5), and $K_y = \begin{bmatrix} k_{y1} & \dots & k_{yn} \end{bmatrix}^T$, $k_{yi} \in \mathbb{R},\ \forall i = 1, \dots, n,$ is the linear vector gain to be conceived.

The slave system (5) generates the output signal $y_s(k)$ and the recovered key $K_r(k)$ used to decrypt $V_r(k)$ and to recover the original plaintext using a decryption rule $Dec(.)$, as following:

$$m_r(k) = Dec\left(\alpha^{-1}V_r(k), -K_r(k)\right) = Enc\left(\alpha^{-1}V_r(k), -K_r(k)\right) = \underbrace{f_1(\dots f_1(}_{q} f_1(\alpha^{-1}V_r(k), \underbrace{-K_r(k)), -K_r(k)), \dots, -K_r(k))}_{q} \quad (6)$$

with:

$$V_r(k) = y_m(k) - y_s(k) \quad (7)$$

and:

$$K_r(k) = \sqrt{x_{s1}^2(k) + \dots + x_{sn}^2(k)} \quad (8)$$

$x_{si}(k),\ \forall i = 1, \dots, n$ are elements of the state vector $x_s(k)$.

Taking into account that the chaotic trajectory remains confined in a bounded space [25], the problem, considered in this paper, is to design a hybrid output feedback, combining both linear and nonlinear control laws. The linear part is independent of the master and slave variables $x_m(k)$ and $x_s(k)$, but the nonlinear one is, essentially, used to set aside the obtained instantaneous function resulting after coupling the slave hyperchaotic system with the master one. Obviously, the developed hybrid output feedback must be determined such that the master and slave synchronization is achieved.

Therefore, it is amount to find suitable scalars $\left(r_i, k_{y_i}\right)$ for $i = 1, \dots, n,$ such that master-slave synchronization defined by:

$$\lim_{k \to +\infty} \left\| x_{mi}(k) - x_{si}(k) \right\| = 0,\ \forall i = 1, \dots, n \quad (9)$$

is fulfilled.

In the next subsection, the design of a hybrid discrete-time output feedback is proposed to synchronize 5 with 1.

B. Proposed hybrid output feedback-based approach for discrete-time hyperchaotic synchronization

In this part, a systematic procedure to synchronize master and slave hyperchaotic systems is proposed [1-2].

By considering the synchronization error vector $e(k)$, such that:

$$e(k) = x_m(k) - x_s(k) \tag{10}$$

the error system between (1) and (5) can be described by:

$$\begin{aligned} e(k+1) &= A_m(.)x_m(k) - A_s(.)x_s(k) \\ &\quad -K_y Ce(k) + \alpha V_t(k)\left(R - K_y\right) \end{aligned} \tag{11}$$

In the particular case where $R = K_y$, then it comes:

$$e(k+1) = A_m(.)x_m(k) - A_s(.)x_s(k) + BU(k) \tag{12}$$

with $B = \mathbb{I}_{n\times n}$.

In fact, for several discrete-time hyperchaotic systems, we have:

$$A_m(.)x_m(k) - A_s(.)x_s(k) = A_c(.)e(k) + G\left(x_m(k), x_s(k)\right) \tag{13}$$

For this reason, let us consider the proposed slightly modified hybrid output feedback $U(k)$ defined by:

$$U(k) = -K_y\left(y_m(k) - y_s(k)\right) - G\left(x_m(k), x_s(k)\right) \tag{14}$$

leading, in this case, to the error system description which can be reduced to the following compact form:

$$e(k+1) = A_c\left(x_m(k), x_s(k)\right)e(k) \tag{15}$$

with:

$$A_c\left(x_m(k), x_s(k)\right) = A_e\left(x_m(k), x_s(k)\right) - BK_yC \tag{16}$$

and $A_c(.) = \left\{a_{cij}(.)\right\}$, $a_{cij}(.) = a_{eij}(.) - k_{y_i}c_j$, $\forall i, j = 1,\ldots,n$.

From the control theory viewpoint, the synchronization of systems (1) and (5) is equivalent to the stabilization of the dynamical error system (12) by a suitable modified output feedback control law $U(k)$ conceived by respect to (14).

To achieve this goal, let us elaborate stability conditions guaranteeing the asymptotic stability of the obtained closed-loop error system, described in the state space, by (15) and (16).

The overvaluing system $M\left(A_c\left(x_m(k), x_s(k)\right)\right)$, associated to the following vectorial norm [14]:

$$p\left(z(k)\right) = \left[\left|z_1(k)\right| \quad \ldots \quad \left|z_n(k)\right|\right]^T \tag{17}$$

with $z(k) = \left[z_1(k) \quad \ldots \quad z_n(k)\right]^T$, is described by:

$$z(k+1) = M\left(A_c\left(x_m(k), x_s(k)\right)\right)z(k) \tag{18}$$

with $M\left(A_c\left(x_m(k), x_s(k)\right)\right) = \left\{m_{ij}(.)\right\}$, $m_{ij}(.) = \left|a_{cij}(.)\right|$, $\forall i, j = 1,\ldots,n.$

Chaotic signals are bounded and generated in a deterministic manner [25]. Exploiting this property, the matrix $M\left(A_c\left(x_m(k), x_s(k)\right)\right)$ can be overvalued by an $n\times n$ matrix $M_o = \left\{m_{oij}\right\}$, $\forall i, j = 1,\ldots,n$, whose all elements are constant, positive and independent of both state variables $x_m(k)$ and $x_s(k)$, of the master and slave systems such that the inequality (19):

$$p(k+1) \le M\left(A_c\left(x_m(k), x_s(k)\right)\right)p(k) \le M_o\,p(k) \tag{19}$$

is verified.

The system (12) is, then, stabilized by (14), if the matrix $\left(\mathbb{I} - M_o\right)$ is an M −matrix, i.e.:

$$\left(\mathbb{I} - M_o\right)\begin{pmatrix} 1 & \ldots & i \\ 1 & \ldots & i \end{pmatrix} > 0 \;\; \forall i = 1,\ldots,n \tag{20}$$

Taking into consideration that the arrow form choice for instantaneous characteristic matrices makes sufficient stability conditions easy to test, let us design the control law $U(k)$, so that the instantaneous characteristic overvaluing matrix of the closed-loop system M_o be under the forced arrow form, such as [18-23]:

$$\begin{cases} e_i(k+1) = m_{oii}e_i(k) + m_{oin}e_n(k), \;\; \forall i = 1,\ldots,n-1 \\ e_n(k+1) = \sum_{i=1}^{n-1} m_{oni}e_i(k) + m_{onn}e_n(k) \end{cases} \tag{21}$$

Then, the following theorem, based on the use of Kotelyanski lemma [18-20] associated to the specific forced arrow form matrix M_o, introduced in (21) [18-23], gives sufficient conditions of complete synchronization, relatively to slave (5) with master (1) systems.

Theorem. The dynamical synchronization error vector (10) converges towards zero, if the matrix M_o, is in the forced arrow form such that:

i. the diagonal elements, m_{oii}, of the constant matrix M_o satisfy:

$$1 - m_{o_{ii}} > 0, \;\; \forall i = 1,\ldots,n-1 \tag{22}$$

ii. there exist $\varepsilon > 0$ for which:

$$\Delta = 1 - m_{onn} - \sum_{i=1}^{n-1}\left(m_{oin}m_{oni}\left(1 - m_{oii}\right)^{-1}\right) > \varepsilon \tag{23}$$

Proof. The error system (15), described by (16), is stabilized by the proposed output feedback control law (14), if we make an appropriate choice of the linear output feedback gain K_y such as the matrix $\left(\mathbb{I} - M_o\right)$ is an M −matrix [18], that is to say:

$$\begin{cases} 1 - m_{oii} > 0, \;\; \forall i = 1,\ldots,n-1 \\ \det\left(\mathbb{I} - M_o\right) \ge \varepsilon > 0 \end{cases} \tag{24}$$

The computation of the first member of the last inequality, announced in (24), leads to the following expression:

$$\det\left(\mathbb{I}-M_o\right)=\Delta\prod_{j=1}^{n-1}\left(1-m_{ojj}\right) \tag{25}$$

and achieves easily the proof of the above-mentioned Theorem.

III. Synchronization of Two Non-Identical Discrete-Time Hyperchaotic Maps Based on Hybrid Output Feedback and its Application to Secure Communication

In this Section, the considered discrete-time hyperchaotic systems are the Baier-Klein map, which can be expressed as [18]:

$$\begin{cases} x_{m1}(k+1)=-x_{m2}^2(k)-0.1x_{m3}(k)+1.76 \\ x_{m2}(k+1)=x_{m1}(k) \\ x_{m3}(k+1)=x_{m2}(k) \\ y_m(k)=2x_{m1}(k)+x_{m2}(k) \end{cases} \tag{26}$$

and the Hitzel-Zele map, which can be expressed as [24-25]:

$$\begin{cases} x_{s1}(k+1)=-0.3x_{s2}(k) \\ x_{s2}(k+1)=-1.07x_{s2}^2(k)+x_{s3}(k)+1 \\ x_{s3}(k+1)=x_{s1}(k)+0.3x_{s2}(k) \\ y_s(k)=2x_{s1}(k)+x_{s2}(k) \end{cases} \tag{27}$$

Remark. The hyperchaotic attractors of master system (26) and slave system (27), Figure 2, with the initial values $x_m(0)=\begin{bmatrix}1 & -1 & 0.5\end{bmatrix}^T$ and $x_s(0)=\begin{bmatrix}1.5 & 0.2 & 0.1\end{bmatrix}^T$ illustrate that state variables $x_{mi}(k)$ and $x_{si}(k)$ are bounded [25], such that: $|x_{mi}|<2,\ |x_{si}|<2,\ \forall i=1,\ldots,3.$

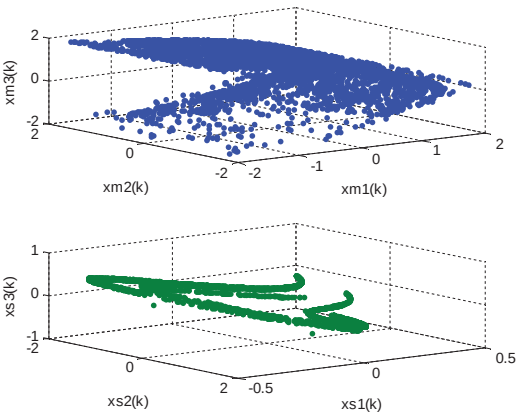

Figure 2. Hyperchaotic attractors of the Baier-Klein and the Hitzel-Zele maps

Let us consider the following master and slave Baier-Klein and Hitzel-Zele hyperchatic systems [18,24-25]:

- the master system:

$$\begin{cases} x_m(k+1)=A_m(.)x_m(k)+\alpha RV_t(k) \\ y_m(k)=Cx_m(k)+\alpha V_t(k) \end{cases} \tag{28}$$

with:

$$A_m(.)=\begin{bmatrix} 0 & -x_{m2}(k) & -0.1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{29}$$

and:

$$C=\begin{bmatrix}2 & 1 & 0\end{bmatrix} \tag{30}$$

- the slave system:

$$\begin{cases} x_s(k+1)=A_s(.)x_s(k)+K_y\left(y_m(k)-y_s(k)\right) \\ y_s(k)=Cx_s(k) \end{cases} \tag{31}$$

with:

$$A_s(.)=\begin{bmatrix} 0 & -0.3 & 0 \\ 0 & -1.07x_{s2}(k) & 1 \\ 1 & 0.3 & 0 \end{bmatrix} \tag{32}$$

and $K_y=\begin{bmatrix}k_{y1} & k_{y2} & k_{y3}\end{bmatrix}^T$, the linear output feedback gain to be found.

Let us consider the synchronization error $e(k)$, between systems (28) and (31):

$$e_i(k)=x_{mi}(k)-x_{si}(k),\ \forall i=1,\ldots,3 \tag{33}$$

Then, it comes the following instantaneous characteristic matrix (16) of the so obtained dynamical error system (33):

$$A_c\left(x_m(k),x_s(k)\right)=\begin{bmatrix} -2k_{y1} & -\left(x_{m2}(k)+k_{y1}\right) & 0 \\ 1-2k_{y2} & -k_{y2} & 0 \\ -2k_{y3} & 1-k_{y3} & 0 \end{bmatrix} \tag{34}$$

such that:

$$G\left(x_m(k),x_s(k)\right)=\begin{bmatrix} x_{s2}(k)\left(-x_{m2}(k)+0.3\right)-0.1x_{m3}(k)+1.76 \\ x_{s1}(k)+1.07x_{s2}^2(k)-x_{s3}(k)-1 \\ -x_{s1}(k)+0.7x_{s2}(k) \end{bmatrix} \tag{35}$$

By the use of the vectorial norm (17), the overvaluing system associated to (34) is characterized by the instantaneous matrix $M\left(A_c\left(x_m(k),x_s(k)\right)\right)$, given by (36):

$$M\left(A_c\left(x_m(k),x_s(k)\right)\right)=\begin{bmatrix} 2|k_{y1}| & |x_{m2}(k)+k_{y1}| & 0 \\ |1-2k_{y2}| & |k_{y2}| & 0 \\ 2|k_{y3}| & |1-k_{y3}| & 0 \end{bmatrix} \tag{36}$$

As it is noted in the above-cited Remark, states variables of the master hyperchaotic system are bounded such as: $|x_{m2}(k)| < 2$; thus, we have:

$$|x_{m2}(k) + k_{y1}| < 2 + |k_{y1}| \quad (37)$$

So, it comes a new overvaluing system characterized by the constant matrix M_o, defined by:

$$M_o = \begin{bmatrix} 2|k_{y1}| & 2 + |k_{y1}| & 0 \\ |1 - 2k_{y2}| & |k_{y2}| & 0 \\ 2|k_{y3}| & |1 - k_{y3}| & 0 \end{bmatrix} \quad (38)$$

A circular permutation on the components of M_o and the choice of the constant parameter k_{y3} as following:

$$1 - k_{y3} = 0 \Rightarrow k_{y3} = 1 \quad (39)$$

makes the matrix (38) under the forced arrow form.

By referring to the proposed Theorem, both synchronization conditions (22) and (23) become:

$$\begin{cases} 1 - |k_{y2}| > 0 \\ 1 - 2|k_{y1}| - \dfrac{|1 - 2k_{y2}|\left(2 + |k_{y1}|\right)}{1 - |k_{y2}|} > 0 \end{cases} \quad (40)$$

From several possibilities relatively to the linear gain matrix K_y, let choose the following one:

$$K_y = \begin{bmatrix} 0.15 & 12.35 & 1.00 \end{bmatrix}^T \quad (41)$$

obtained by using fmincon instruction of Matlab, in order to consider the most optimized linear gain matrix K_y.

This constant gain matrix will be used, in the next Section, to test a secure signal transmission.

IV. Simulation Results and Comments

The efficiency of the proposed method for designing the adapted hybrid output feedback together with various numerical simulations studies are presented in this Section.

From Figure 3., one can see that the responses of master system (28) and slave system (31), obtained when the control is turned off, show that both states are not yet synchronized. To overcome this, the third order Baier-Klein and Hitzel-Zele maps synchronization is applied using the gain K_y given in (41) for initial conditions of master system (28) and slave system (31): $\left(x_m(0), x_s(0)\right) = \left(\begin{bmatrix} 1 & -1 & 0.5 \end{bmatrix}^T, \begin{bmatrix} -0.5 & 0.2 & 0.3 \end{bmatrix}^T\right)$.

Figure 4. illustrates the effectiveness of the proposed method based on the use of aggregation techniques associated to the forced arrow form matrix for system description.

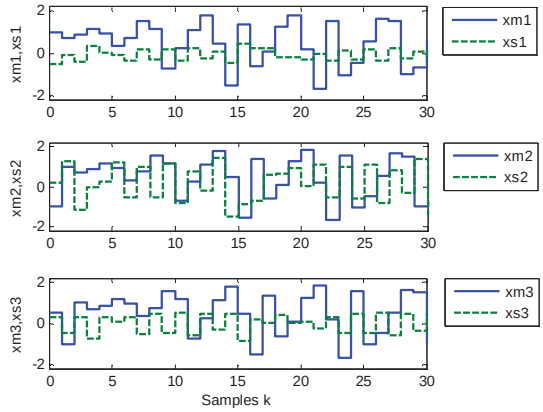

Figure 3. Evolutions of the master and slave Baier-Klein and Hitzel-Zele maps state responses when controller is switched off

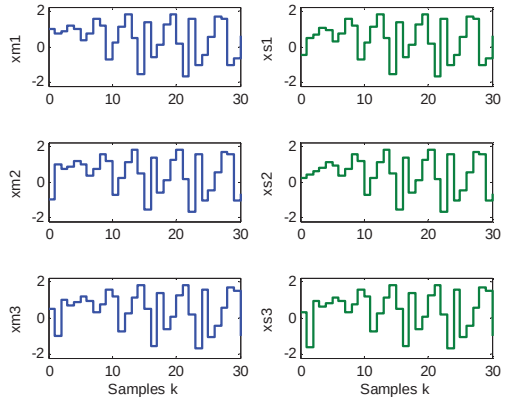

Figure 4. Time responses of spatiotemporal chaos synchronization of master Baier-Klein and slave Hitzel-Zele state variables

For the encryption $h = 2$, $\alpha = 0.01$, $q = 5$ and the sampling time $T = 0.01\ s$, the hyperchaotic signal of the transmitter, including information signal $m_t(k)$, $m_t(k) = \sin\left(0.3k\right)$, is sent to the receiver and the information signal $m_r(k)$ is recovered approximately by the proposed output feedback as shown in Figure 5. (a). and Figure 5. (b).

$y_m(k)$, sent in the public channel between the transmitter and the receiver, is given in Figure 5. (e). and the obtained transmitter and receiver keys, respectively in, Figure 5. (c). and Figure 5. (d).

One can observe that precisely, when the master and slave systems are synchronized i.e., $x_s(k) \to x_m(k)$; it follows $K_r(k) \to K_t(k)$, $V_r(k) \to V_t(k)$ as $k \to +\infty$.

To avoid the distortion of the recovered messages $m_r(k)$, at transient regime, a solution is to transmit an adapted delayed $m_t(k)$.

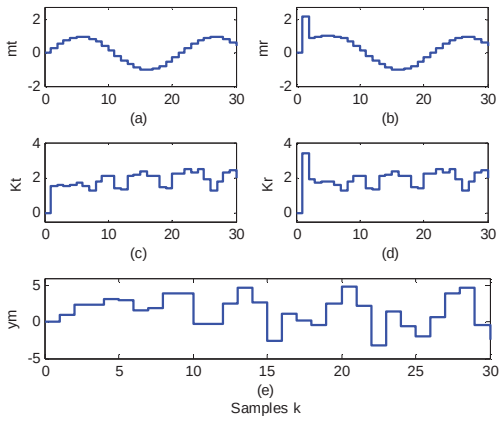

Figure 5. An example of hyperchaotic cryptography using the 3D Baier-Klein and Hitzel-Zele maps

V. CONCLUSION

In this paper, a hybrid output feedback controller for the synchronization of wide class of discrete-time hyperchaotic systems via a transmitted signal is designed. The design is based on the use of aggregation techniques for convergence study and forced arrow form matrix for system description. Conventional cryptographic methods and synchronization of hyperchaotic systems have been combined in order to design efficient hyperchaotic-based secure communication systems. The validity of the proposed synchronization and secure communication scheme is confirmed by numerical simulation results when third order Baier-Klein and Hitzel-Zele maps are used. Finally, it is worth pointing out that the problem of improving time synchronization is a challenging one and will be investigated in a future work.

REFERENCES

[1] L. M. Pecora, T. L. Carroll, "Synchronization in chaotic systems", Physics Revue Letters, vol. 64, n° 8, pp. 821-824, 1990.

[2] T. L. Carroll, L. M. Pecora, "Synchronizing chaotic circuits", IEEE Transactions on Circuits and Systems, vol. 38, n° 4, pp. 453-456, 1991.

[3] I.Belmouhoub, M. Djemaï, J.P. Barbot, "Cryptography by discrete-time hyperchaotic systems" IEEE-CDC, Proceedings of the 42nd IEEE Conference on Decision and Control, vol. 2, pp. 1902-1907, 2003.

[4] M. Djemaï, J.P. Barbot, D. Boutat, "New type of data transmission using a synchronization of chaotics systems" International Journal of Bifurcations and Chaos, vol. 15, n° 1, pp. 1-17, 2005.

[5] I. Belmouhoub, M. Djemaï, "Synchronization of discrete-time chaotic systems for secured data transmission", in Chaos in Automatic Control: From Theory Towards Engineering Application, Edited by W. Perruquetti and J.P. Barbot, CRC Press Book, pp. 527-551, 2005.

[6] R. Kharel, K. Busawon, Z. Ghassemlooy, "Secure digital communication using discrete-time chaotic systems via indirect coupling synchronization", in American Control Conference, Baltimore, Maryland, USA, 2010.

[7] Y. Uyaroğlu, I. Pehlivan, "Nonlinear Sprott94 case a chaotic equation: synchronization and masking communication applications", Computers and Electrical Engineering, vol. 36, n° 6, pp. 1093-1100, 2010.

[8] Ö. Morgül, M. Feki, "A chaotic masking scheme by using synchronized chaotic systems", Physics Letters A, vol. 251, n° 3, pp. 169-176, 1999.

[9] S. Bowonga, F. M. Kakmenib, M. S. Siewe, "Secure communication via parameter modulation in a class of chaotic systems", Communication in Nonlinear Science and Numerical Simulations, vol. 12, n° 3, pp. 397-410, 2007.

[10] K. Fallahi, H. Leung, "A chaos secure communication scheme based on multiplication modulation", Communication in Nonlinear Science and Numerical Simulations, vol. 15, n° 2, pp. 368-383, 2010.

[11] H. Dedieu, M. P. Kennedy, M. Hasler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using selfsynchronizing chua's circuit", IEEE Transactions on Circuits and Systems II: Analog Digital Signal Process, vol. 40, n° 10, pp. 634-642, 1993.

[12] W. Liu, Z. Wang, M. Ni, "Controlled synchronization for chaotic systems via limited information with data packet dropout", Automatica, vol. 49, n° 8, pp. 2576-2579, 2013.

[13] G. Grassi, D. A. Miller, "Theory and experimental realization of observer-based discrete-time hyperchaos synchronization", IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 49, n° 3, pp. 373-378, 2002.

[14] G. Millerioux, J. Daafouz, "An observer-based approach for input-independent global chaos synchronization of discrete-time switched systems", IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 50, n° 10, pp. 1270-1279, 2003.

[15] G. P. Jiang, W. K. S. Tang, G. Chen, "A simple global synchronization criterion for coupled chaotic systems", Chaos, Solitons and Fractals, vol. 15, n° 5, pp. 925-935, 2003.

[16] G. Grassi, D. A. Miller, "Dead-beat full state hybrid projective synchronization for chaotic maps using a scalar synchronizing signal", Communication in Nonlinear Science and Numerical Simulations, vol. 17, n° 4, pp. 1824-1830, 2012.

[17] T. L. Liao, S. H. Tsai, "Adaptive synchronization of chaotic systems and its application to secure communication", Chaos, Solitons and Fractals, vol. 11, n° 9, pp. 1387-1396, 2000.

[18] S. Hammami, "Hybrid synchronization of discrete-time hyperchaotic systems based on aggregation techniques for image encryption", in the IEEE 14th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering, Sousse, Tunisia, pp. 325-330, 2013.

[19] S. Hammami, K. Ben Saad, M. Benrejeb, "On the synchronization of identical and non-identical 4-D chaotic systems using arrow form matrix", Chaos, Solitons and Fractals, vol. 42, n° 1, pp. 101-112, 2009.

[20] S. Hammami, M. Benrejeb, M. Feki, P. Borne, "Feedback control design for Rössler and Chen chaotic systems anti-synchronization", Physics Letters A, vol. 374, n° 28, pp. 2835-2840, 2010.

[21] S. Hammami, M. Benrejeb, "Coexistence of synchronization and anti-synchronization for chaotic systems via feedback control", Chaotic Systems, Croatia: Editions INTECH, pp. 203-224, 2011.

[22] S. Hammami, "Secure image transmission via nonlinear observer-based chaotic synchronization", Archives Des Sciences, vol. 66, n° 7, pp. 100-115, 2013.

[23] S. Hammami, "Security analysis of high dimensional chaotic-based cryptosystem via its key sensitivity study", Journal of Information Security Research, vol. 4, n° 4, pp. 183-194, 2013.

[24] X. S. Yang, "Concepts of synchronization in dynamical systems", Physics Letters A, vol. 260, n° 5, pp. 340-344, 1999.

[25] G. Baier, M. Klein, "Maximum hyperchaos in generalized Hénon circuit", Physics Letters A, vol. 151, n° 67, pp. 281-284, 1990.

[26] I.Belmouhoub, M. Djemaï, J.P. Barbot, "Observability quadratic normal forms for discrete-time systems" IEEE Transactions on Automatic Control, vol. 50, n° 7, pp. 1031-1038, 2005.

[27] M. Djemaï, J.P. Barbot, I. Belmouhoub, "Discrete time normal form for left invertibility problem", in EJC Issue, in European Journal of Control, vol. 15, n° 2, pp. 194-204, 2009.